AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0020.1] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes fetch logic, translation logic, and execution logic. The fetch logic is disposed within a microprocessor and is configured to receive a cryptographic instructionsingle atomic cryptographic instruction as part of an instruction flow executing on the microprocessor. The ~~cryptographic instruction~~single atomic cryptographic instruction prescribes one of the cryptographic operations, and also one of a plurality of data block sizes. The translation logic is coupled to the fetch logic, and is configured to translate the single atomic cryptographic instruction into a sequence of micro instructions that directs the microprocessor to perform the one of the cryptographic operations. The execution logic is disposed within the microprocessor and is operatively coupled to the ~~cryptographic instruction~~single atomic cryptographic instruction. The execution logic executes the one of the cryptographic operations. The execution logic ~~has a block size~~ controller that employs the one of a plurality of data block sizes during execution of the ~~one of the cryptographic operations~~includes a cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, where the one of a plurality of data block sizes is prescribed by a control word that is provided to a block size controller within the cryptography unit, and where the block size controller employs the one of a plurality of data block sizes during execution of the one of the cryptographic operations.

[0021] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has a cryptography unit disposed within execution logic in within a microprocessor and block size logic. The cryptography unit

executes one of the cryptographic operations responsive to receipt by the microprocessor of a cryptographic instructionsingle atomic cryptographic instruction within an instruction flow that prescribes the one of the cryptographic operations. The ~~cryptographic instruction~~single atomic cryptographic instruction is fetched from memory by fetch logic in the microprocessor. The cryptographic instructionsingle atomic cryptographic instruction also prescribes a block size to be employed when executing the one of the cryptographic operations. Translation logic in the microprocessor translates the single atomic cryptographic instruction into a sequence of micro instructions that directs the microprocessor to perform the one of the cryptographic operations. The block size logic is operatively coupled within the cryptography unit. The block size logic directs the device to employ the block size when performing the one of the cryptographic operations.

[0022] Another aspect of the present invention provides a method for performing cryptographic operations in a device. The method includes, within a microprocessor, fetching a cryptographic instructionsingle atomic cryptographic instruction from memory that prescribes employment of particular data block size during execution of one of a plurality of cryptographic operations, and translating the single atomic cryptographic instruction into a sequence of micro instructions that direct the microprocessor to perform the one of the plurality of cryptographic operations; and, via a cryptography unit disposed within execution logic in the microprocessor, within the microprocessor, executing the ~~cryptographic instruction and~~ employing the particular data block size when performing the one of the cryptographic operations.

Kindly replace paragraph [0012] with the following amended paragraph:

[0012] To perform cryptographic operations on multiple successive blocks of text, all of the symmetric key algorithms employ the same types of modes. These modes include electronic code book (ECB) mode, cipher block chaining (CBC) mode, cipher feedback (CFB) mode, and output feedback (OFB) mode. Some of these modes utilize an additional initialization vector during performance of the sub-operations and some use the ciphertext output of a first set of cryptographic rounds performed on a first block of

plaintext as an additional input to a second set of cryptographic rounds performed on a second block of plaintext. It is beyond the scope of the present application to provide an in depth discussion of each of the cryptographic algorithms and sub-operations employed by present day symmetric key cryptographic algorithms. For specific implementation standards, the reader is directed to Federal Information Processing Standards Publication 46-3 (FIPS-46-3), dated October 25, 1999 for a detailed discussion of DES and Triple DES, and Federal Information Processing Standards Publication 197 (FIPS-197), dated November 26, 2001 for a detailed discussion of AES. Both of the aforementioned standards are issued and maintained by the National Institute of Standards and Technology (NIST) and are herein incorporated by reference for all intents and purposes. In addition to the aforementioned standards, tutorials, white papers, toolkits, and resource articles can be obtained from NIST's Computer Security Resource Center (CSRC) over the Internet ~~at http://csrc.nist.gov~~.